Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Layer-7 Secure Security Posture

This paper intends on applying the lessons learned from the lower levels of the OSI model to the upper layers. The following figure shows the OSI model. The seven layers are also looked at as two groups of layers - Application and Data Transport layers. It is within the boundary between the application and data transport layers that we cross the philosophical split on whether your site needs to take a "default deny" or a "default permit" stance. End users and system administrators wholeheartedly believe that anything t...

Copyright SANS Institute
Author Retains Full Rights

AD

A Layer-7 Secure Security Posture

Paul Vinciguerra
November 17, 2001

Lessons learned from layers 4 and below

I find it interesting how guiding principles don't survive across IT disciplines. Take, for example, the concept of a security stance – your site's attitude toward security. The two fundamental postures are the secure, "default deny" and the reactive, "default permit" stances. In the "default deny" stance, you specify only what you allow and deny the rest, wherein with the "default permit" stance, the opposite is true; you specify only what you prohibit and allow the rest. The shortcoming of the default permit stance, of course, is that you must know what you need to deny prior to the exposure.

Network engineers and designers who have any experience with network security recognize the need to understand your traffic flow, and then specifically allow the traffic you need and deny the rest. Network designers implement these controls, commonly referred to as ACLs (Access control lists) on access routers or firewalls. The ACLs provide highly granular controls based on transport layer information – ip addresses, protocols like ICMP(Protocol 1), TCP(Protocol 6), UDP(Protocol 17), and in the case of TCP, additional granularity can be further achieved by examining the TCP flags.

This paper intends on applying the lessons learned from the lower levels of the OSI model to the upper layers. The following figure shows the OSI model. The seven layers are also looked at as two groups of layers – Application and Data Transport layers. It is within the boundary between the application and data transport layers that we cross the philosophical split on whether your site needs to take a "default deny" or a "default permit" stance. End users and system administrators wholeheartedly believe that anything that hasn't clearly been prohibited should be fair game, while network engineers intuitively see the need for the "default deny" stance.

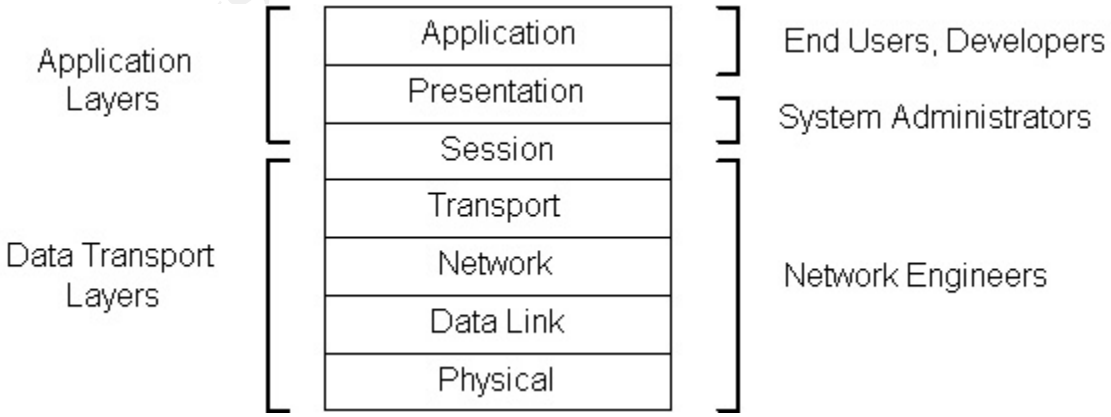

Figure 1- 2 sets of layers that make up the OSI model[1]

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The OSI model needs to be looked at in a client-server environment to make the concepts gel. Taking for a moment a typical web server interaction, a client application—a browser, a search engine's c-program or a hacker's perl script makes a request to big-server.com. The application layer passes the request on to the presentation layer, where cross-platform compatibility is ensured. A browser on an ASCII based PC can access data as seamlessly on an EBCDIC Mainframe as on an Intel PC. As the presentation layer formats the request into the proper data format, the length of the request may either increase or decrease. The request moves onto the session layer. This is where the service requests and responses exist whole from the applications perspective. As it moves down to the transport layer, the transport layer takes care of managing the communication between hosts. This is where the concept of virtual circuits and sockets appear. The session layer information may be broken up into multiple transport-layer data-units in a way to facilitate reassembly by the host on the other side. The maximum sized of these transport-layer data-units is known as the MSS (Maximum Segment Size) and is a kernel tunable parameter on Unix platforms. As each transport-layer data-unit moves down to the network layer, the network layer adds logical hierarchical addressing so that an optimum path to end-host can later be traversed. Here once again, the network layer may need to break up the transport-layer data-unit into multiple network-layer data-units. The network data-units move down to the data-link layer where physical addressing is determined of the next-hop host, whether it is an intermediary or the end-host. Once again, here the upper layer packets, the network-layer data-units may need to be broken up to support the maximum size of the data link layer, often called the MTU (Maximum transition unit). The MTU is often calculated for each session by what is known as the path MTU, which is equal to the smallest MTU of any segment along the packet's path and may change within a session should the data need to traverse another path. Intermediary hosts, such as routers, will fragment packets going from media with a larger MTU to a smaller MTU. They will not however, reassemble packets; this is left for the end host.

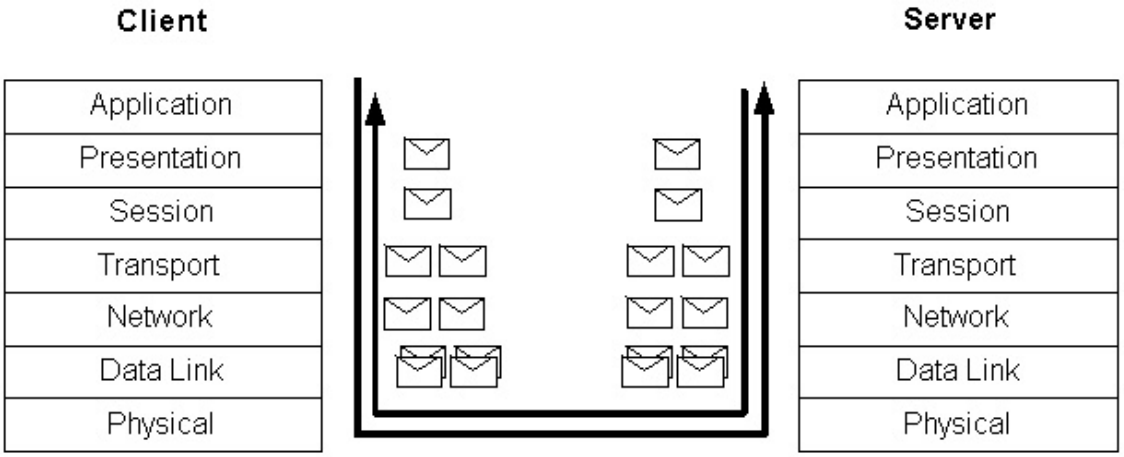

Figure 2 - The OSI Model in a client-server environment

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

What happens in practice is that at the lower levels, the security conscious network or security engineer will attempt to monitor and detect (and possibly shun) an invalid application request that may be in any valid format that their server's presentation layer may accept. This is compounded by the need to collect and rebuild the application layer request from many physical layer packets. Unfortunately, if the request were in say, 20 packets, it could be possible to hide the attack from the IDS until the 20th. packet had been transmitted and only if the IDS were able to do packet reassembly. In this case, the IDS would be determining the malicious code at the same time it were being run on the target machine. At best, it could shun an individual machine from accessing the now compromised server.

In the case of web servers, this application-to-application interaction is where a large number of exploits occur today. Code Red, Code Blue, NIMDA, and directory traversal exploits lead the pack in application layer exploits – mainly against Microsoft IIS. The Gartner group has now recommended that organizations move away from the use of IIS.[2] However, In a poll of systems administrators by windows 2000 magazine, 26% of those polled planned to migrate to Apache, while 53% sited they would "not change--you need Microsoft technology"[3]

Unfortunately, this sentiment is compounded by the opinions of many CEO's that there is nothing of value on their web servers and thus not a great need to secure these servers.[4] What is often overlooked is that on these servers is the privilege to access the data of value. The use or misuse of that privilege, once the server has been compromised can be used to penetrate the firewalls as these types of communications are permitted as a matter of design.

These application layer exploits are an old problem resurfacing in newer applications. Another example of these application layer issues can be found dating back to 1994 with sendmail, another application with a rich history of security issues can be found in William Cheswick and Stephen Bellovin. Firewalls and Internet Security. Repelling the Wily Hacker.

> A recent *sendmail* bug provides a sterling example. Problems with certain mail header lines could tickle bugs in delivery agents. Our firewall, and many others, paid almost no attention to headers, believing that they were strictly a matter for mail readers and composers (known as user agents in the e-mail biz) But that meant that the firewalls provided no protection against this problem, because under certain circumstances, *sendmail*—which is run on many internal machines here—does look at the headers, and certain entries made it do evil things.
>
> Furthermore, even if we had implemented defenses against the known flaws, we would still be vulnerable to next year's. If someone invented a new header line that was implemented poorly—and this particular problem did involve a nonstandard header –we would still be vulnerable. We could have protected

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

> ourselves if and only if we had refused to pass anything but the minimal subset of headers we did know of, and even then there might have been danger if some aspect of processing a legitimate, syntactically correct header was implemented poorly. At best, a firewall provides a convenient single place to apply a corrective filter.[5]

The extension and application of the lower network-level controls in place at most organizations need to move to the upper layers. We need to bring to the application layer, the concept of the "default deny" stance, in which you specify only what you allow and deny the rest.

Enter the ALG

Cisco recognized the need for this type of proactive screening and introduced application layer protection for SMTP into the enterprise with the introduction of Mailguard on their PIX firewalls[6]. Mailguard screens all inbounds SMTP requests and allows only seven "safe" commands to be passed into the SMTP gateway. These seven "safe" commands are: HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT. Unfortunately, Mailguard has not kept up with the times and these days provides less security by defeating the ESMPT commands like STARTTLS which will transmit the email message over the internet encrypted within an SSL/TLS session.

In the PIX solution, there typically is no independent bastion host. The PIX will have a static NAT entry inbound to the mail server sitting on the internal network and is typically configured by the following code snippet:

```
fixup protocol smtp 25
static (inside,outside) <external Address> <Mailhost Internal Address>
access-list inbound permit tcp any host mailhost eq smtp
```

Turning off mailguard can be accomplished by the following command entered on the PIX CLI.

```
No fixup protocol smtp 25
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

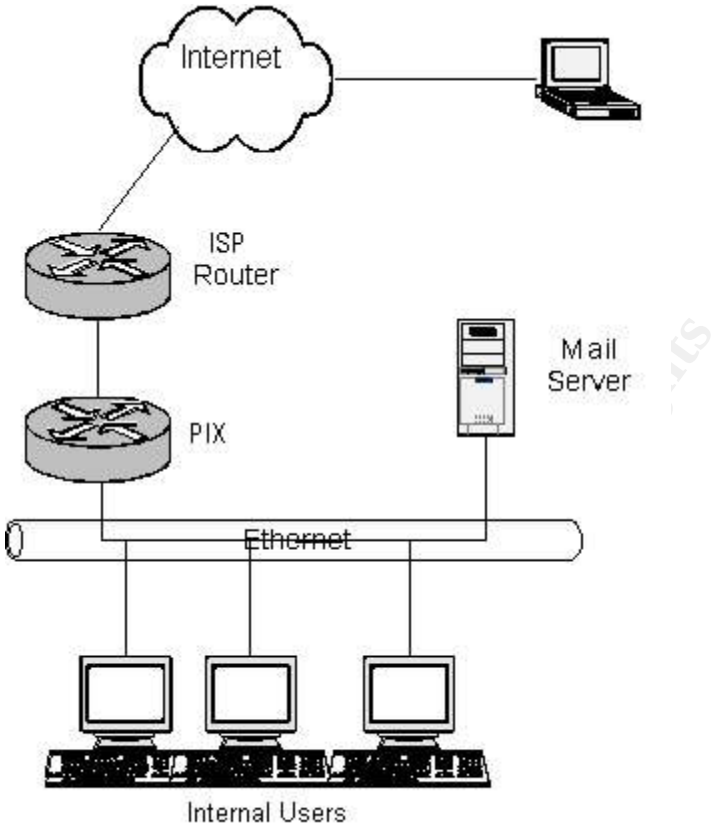

Figure 3- Typical Small office configuration

The typical small office configuration shows how dangerous worms like nimda are.

In a typical exchange server configuration, the exchange server is typically direct on the internal network. The firewall, labeled PIX, is configured to allow all traffic outbound. Inbound, it permits mail delivery via SMTP (TCP/25) and outlook web access (TCP/80). The internal users want to use the outlook client on their desktops and need to be able to establish RPC connections to the exchange server.

Cisco offers Network-Based Application Recognition (NBAR) in IOS versions starting with 12.1.5T for routers other than the 1600[7]. NBAR provides for URL matching for making policy and quality-of-service decisions. NBAR can be used to block URLs, but has many limitations. Most notably, it cannot match more than 24 URLs, parse beyond the first 400 bytes of the URL, handle fragmentation of the URL, or HTTP connection pipelining as in HTTP 1.1. These limitations preclude using NBAR for maintaining a secure posture. It does provide for a mechanism to prevent specific threats while a patch becomes available. Cisco provides detailed instructions on using this feature for blocking code red.[8]

Microsoft also now offers urlscan, a tool that validates URLs before being passed onto IIS.[9] Urlscan is a step in the right direction. Unfortunately, it works as a preprocessor on

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

the IIS server. This model does not leverage the gains from defense in depth found in an n-tier architecture.

The concept of a separate layer-7 bastion host, in which only accept "valid" requests seems a much more logical solution. In a typical bastion host environment, a screening router filters allowed types of network traffic to the bastion host as its destination. The bastion host then in a new network session forwards the request into a server farm protected by another screening router or firewall.

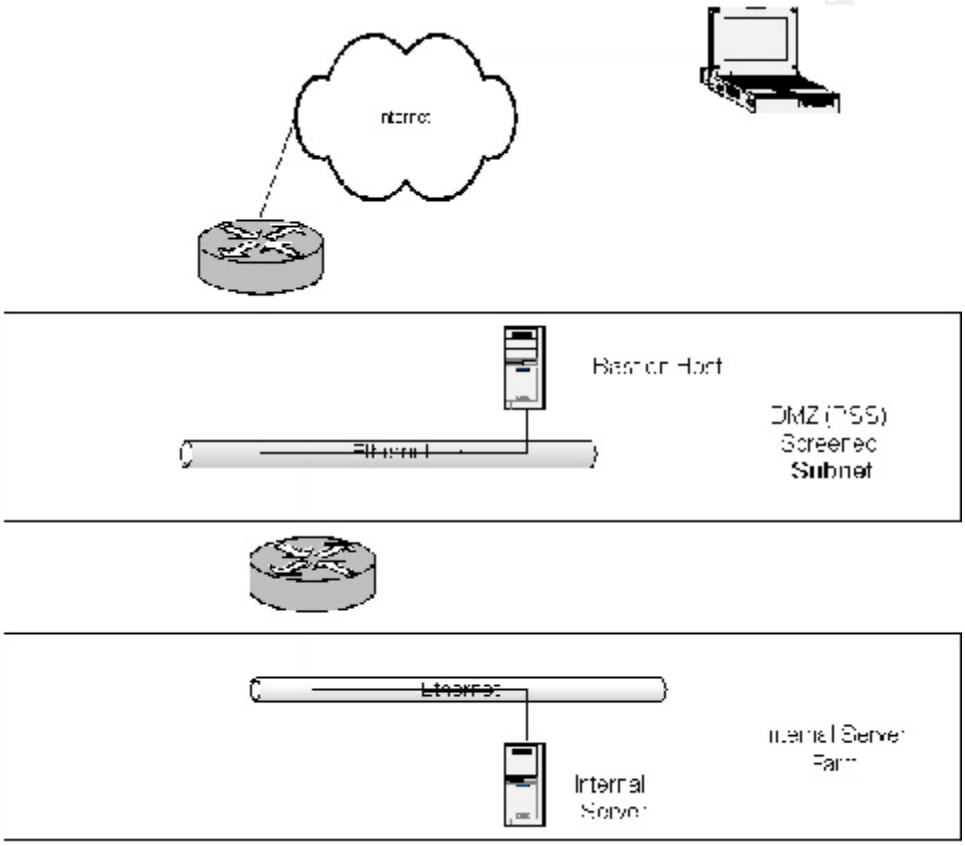

Figure 4- Typical bastion host configuration

This is a strong security stance based on defense-in-depth, supported by most application server vendors.

Vendor	Apache Module
ATG Dynamo	Mod_dynamo
BEA Weblogic	Mod_wl
IBM Websphere	mod_ibm_app_server
Apache Tomcat	Mod_jserv
	Mod_jk
	Mod_webapp

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

In each case, the end user interacts with the bastion web server. URL-to-application mappings in the web server configs direct separate connections in through the internal router/firewall. Examples of these configurations are provided from various vendors below:

Using mod_dynamo, this is accomplished with the following configuration parameter in apache's httpd.conf file.

```
DynamoManager   dynappsvr 8880
```

Using mod_wl[10], the following would be added to the httpd.conf file

```
WebLogicHost myweblogic.server.com
WebLogicPort 7001
MatchExpression *.jsp
```

Using mod_jk, for tomcat, this is accomplished via two configuration files:

Tomcat-apache.conf

```
JkMount /servlet/* ajp13
```

workers.properties

```
worker.list=ajp12,ajp13

worker.ajp12.port=8008
worker.ajp12.host=tomcatsvr
worker.ajp12.type=ajp12

worker.ajp13.port=8009
worker.ajp13.host=tomcatsvr
worker.ajp13.type=ajp13
```

In each case,

What If?

What if we had a mod_iis_proxy module that allowed us to filter incoming requests and only pass through "valid" urls? Let's take a look at applying this model of discerning only valid "permitted" URLs to apache logfile analysis.

```
[pvinci@agertag httpd]$ cat access_log
127.0.0.1 - - [09/Oct/1994:10:48:50 -0400] "GET /index.html HTTP/1.0" 200 2511
127.0.0.1 - - [09/Oct/1994:10:48:52 -0400] "GET /manual/index.html HTTP/1.0" 404 275
127.0.0.1 - - [09/Oct/1994:11:54:43 -0400] "GET /bookmark/favicon.ico HTTP/1.0"404 278
127.0.0.1 - - [09/Oct/1994:11:56:07 -0400] "GET /bookmark/index.html HTTP/1.0" 404 277
127.0.0.1 - - [09/Oct/1994:12:15:59 -0400] "GET /index.html?name=pv HTTP/1.0" 200 2511
127.0.0.1 - - [09/Oct/1994:12:16:20 -0400] "GET /bookmark/index.html?name=pv HTTP/1.0"
404 277
```

First, we can create a rough list of valid URLs for our web server, stripping out the query string and session IDs which may follow in our request.

```
# grep " 200 " access_log | awk -F" " '{print $6 $7}'|awk -F"?" `{print $1}`| \
awk -F";"`{print $1}` |sort | uniq > urls.valid
```

This resulted in just index.html. I added some extra URLs for the test.

```
[pvinci@agertag httpd]$ cat urls.valid
/index.html
/default.html
/index.htm
```

The output of which will be all requests that were unexpected can be inspected via:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
[pvinci@agertag httpd]$ fgrep -v -w -f urls.valid access_log
127.0.0.1 - - [09/Oct/1994:10:48:52 -0400] "GET /manual/index.html HTTP/1.0" 404 275
127.0.0.1 - - [09/Oct/1994:11:54:43 -0400] "GET /bookmark/favicon.ico HTTP/1.0"404 278
127.0.0.1 - - [09/Oct/1994:11:56:07 -0400] "GET /bookmark/index.html HTTP/1.0" 404 277
127.0.0.1 - - [09/Oct/1994:12:16:20 -0400] "GET /bookmark/index.html?name=pv HTTP/1.0"
404 277
```

The output of which will be all requests that were expected can be inspected via:

```
[pvinci@agertag httpd]$ fgrep -w -f urls.valid access_log
127.0.0.1 - - [09/Oct/1994:10:48:50 -0400] "GET /index.html HTTP/1.0" 200 2511
127.0.0.1 - - [09/Oct/1994:12:15:59 -0400] "GET /index.html?name=pv HTTP/1.0" 200 2511
[pvinci@agertag httpd]$
```

It seems to be a viable strategy.

Please note: You need to exercise due care in screening the urls.valid file. On a compromised web server, you may find entries for root.exe, cmd.exe and many other confidential files may be found with 200 status codes.

But now we still need to rebuild the server from scratch…

Ok, we did everything we could to protect our servers. We have an external screening router configured to allow the Internet access to our server on port 80. Our IDS is monitoring the incoming requests. We are monitoring our log files for all invalid URLs and they are being emailed in near real-time.

Even so, the Nimda virus has compromised our server.

Unfortunately, looking at log files is a reactive process, and at best will only point us in the direction of machines that need to be rebuilt from scratch. To work proactively we need to stop the request before it compromises the server.

For something more useful, we need to provide this filtering in real-time.

A Proactive approach — Enter the Layer –7 Strong security posture

Unfortunately, mod_iis_proxy does not exist. However, two apache modules that will provide similar functionality already exist, mod_proxy and mod_eaccess. Assuming we build a bastion host with apache, and these modules, we move toward being able to implement our layer-7 secure security posture. This posture will allow us to stop unauthorized requests (invalid urls) in real time, due to the serial nature of the protection. With this architecture, the end host only receives valid packets once fully validated by the proxy. This is very much different from the use of a shunning IDS where the end host and the IDS receive the packets simultaneously and letting the IDS shun (send a TCP RST) to the hosts to force closed the TCP connection. The success of protection from a shunning IDS is predicated on the assumption that the IDS will be able to detect and terminate the TCP connection before the malicious code reaches the target host.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Mod_proxy is part of the standard apache package, but is not enabled by default. Mod_eaccess can be found at http://httpd.apache.org/dist/httpd/contrib/modules/1.3/ in the file apache-contrib-1.0.8.tar.gz .

Let's build apache with mod_proxy and mod_eaccess for our layer-7 bastion host.

```
[pvinci@agertag sans]$ls
apache-contrib-1.0.8.tar.gz  apache_1.3.20.tar.gz
[pvinci@agertag sans]$gzip -d apache-contrib-1.0.8.tar.gz | tar -xvf -
[pvinci@agertag sans]$gzip -d apache_1.3.2.tar.gz | tar -xvf -
[pvinci@agertag sans]$cd apache_1.3.20

[pvinci@agertag apache_1.3.20]$ ./configure \
   --prefix=/home/pvinci/sans/apache_alg \
   --enable-module=rewrite \
   --enable-shared=rewrite \
   --enable-module=proxy \
   --enable-shared=proxy \
   --add-module=../apache-contrib-1.0.8/mod_eaccess/mod_eaccess.c \
   --enable-shared=eaccess

Configuring for Apache, Version 1.3.20
[pvinci@agertag apache_1.3.20]$make
[pvinci@agertag apache_1.3.20]$ su -c "make install"
Password: XXXXXXX
```

Adding the following code snippet to the httpd.conf file will enable the use of mod_proxy and mod_eaccess with the ruleset found in the file eaccess_acls.

```
ProxyRequests On
ProxyRemote * http://intsvr

ProxyPass / http://intsvr/
ProxyPassReverse / http://intsrv/

# EAccess Directives
EAccessEnable on

EAccessLogLevel 1

EAccessLog logs/eaccess_log
EAccessCache logs/eaccess_auth
EAccessOptim 0

include conf/eaccess_acls
```

Configuration parameters for mod_eaccess can be found here.
Configuration parameters for mod_proxy can be found here.

A starting point for eaccess_acls would be to build a file from your access_log

```
[pvinci@agertag logs]$ cat earules.sh
#!/bin/sh
cat urls.valid | while read i
   do
     echo 'EAccessRule permit "^'$i'$"'
   done
[pvinci@agertag logs]$ grep " 200 " access_log | awk -F" " '{print $6 " " $7}'| sed -e
's/"//g' |sort | uniq >urls.valid


[pvinci@agertag logs]$sh earules.sh >../conf/eaccess_acls


[pvinci@agertag apache_alg]$ cat conf/eaccess_acls
EAccessRule permit "^GET /index\.html$"
EAccessRule permit "^GET /newlook/home\.htm$"
EAccessRule permit "^GET /aboutsans\.htm$"
EAccessRule deny "^GET /.*$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
[pvinci@agertag apache_alg]$
```

A major benefit of this type of application layer filtering is that it allows for systems administrators and developers to get involved in the security process. Without the involvement and commitment of the systems administrators and the developers, these tools cannot provide a layer-7 secure security posture. For this to work, this community has to remain disciplined and implement a secure posture, one in which we permit what is valid and deny the rest.

Shortcomings/Known Issues

Since the proxy method requires the entire packet stream to be rebuilt by the bastion host prior to validation and being passed onto the internal server, this process can add latency to the client side replies. This increased latency is a matter of the serial design.

Mod_proxy is an HTTP 1.0 proxy. RFC 3143 explains the known HTTP Proxy/Caching Problems.[11] Mod_proxy has added HTTP 1.1 support in the form of the VIA header option, which is configurable in the httpd.conf file. The major difference from a protocol level is that in HTTP1.1 multiple requests are multiplexed/demultiplexed over a single TCP connection. This is contrasted against the HTTP 1.0 protocol, in which each request requires it's own TCP connection along with it's associated initialization overhead.

Assuming a client's need to request 4-8 simultaneous elements, there become constraints on the number of simultaneous connections that can be supported. Most kernels today allocate 1-8 KB per socket connection. Assuming the proxy has sufficient memory for these connections, the number of available ephemeral ports becomes a constraining factor for high volume servers. By default, ephemeral port ranges for Linux are 1024-65535(64511 socket connections) and for Solaris are 32768-65535(32767 socket connection). Resources become constrained by the number of TCP connections available to the proxy server to communicate to the inside host.

	Solaris 32768	Linux 64511
4	8192	16128
5	6554	12902
6	5461	10752
7	4681	9216
8	4096	8064

Maximum number of connections based on
the average number of GETs per HTTP 1.1 connection

The starting ephemeral port for Solaris can be decreased from 32768 to 1024 using ndd or the nddconfig script.

```
ndd -set /dev/tcp tcp_smallest_anon_port 1024
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Sun provides the startup script, nddconfig[12] in which the tcp_smallest_anon_port can be set.

```
tcp_smallest_anon_port=1024
```

The number of IIS servers needing these levels of connections is very low. Most servers are more likely to be a company's informational web presence or web-based email access. For these purposes, these numbers are acceptable.

Conclusion

There are two fundamental security postures. They are the secure "default deny" and the reactive "default permit" stances. Typically network engineers see the need for the default deny posture while end users and developers prefer permitting anything "not dangerous".

Deploying a proactive layer-7 secure security posture through use of a layer-7 bastion host that can screen URLs in the same manner as a firewall screens network packets can provide protection against existing and future IIS exploits. This can be implemented to protect IIS servers in an industry standard manner using the classic n-tier architecture by using apache, mod_proxy and mod_eaccess providing defense-in-depth. Mod_eaccess is a very powerful, flexible tool that can be used to filter incoming requests in a manner analogous to configuring rules on a network-level firewall.

Senior management must be convinced that there is the need to protect their web servers. The notion that these servers have nothing of value needs to be dispelled.

The involvement of system administrators and developers in implementing and managing the mod_eaccess rules in a secure stance will benefit the organization through their heightened security awareness and we should eventually begin to expect to see these principles integrated into future revisions of programs and system configurations.

Appendix A: Sample Eaccess examples using regex (Regular Expressions)

Using regular expressions requires understanding of the regex meta characters. These characters are placeholders to indicate formatting within the search string. The use of these meta characters need to be "escaped" by a preceeding \ to match "index.html", you would use "^index\.html$"

Meta Character	Description
^	Beginning of the line
$	End of the line
*	0 or more occurrences of preceding string
+	1 or more occurrences of preceding string
?	0 or 1 occurrences of proceeding string

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

.	Matches any single character
[]	Matches any on the enclosed characters e.g. ca[tr] matches cat and car.
()	Grouping – (ei)+o matches eieio
regexp1|regexp2	Matches regex1 or regex2
char{min,max}	X\{1,3\} matches X, XX, XXX .\{1,3\} matches any 1-3 characters

Table 1 - Regex Meta characters and their associated meanings

To match index.html with no query string could be written as

```
EAccessRule permit "^GET /index\.html$"
```

To match index.html with no regard to what follows the filename, we can omit the trailing $

```
EAccessRule permit "^GET /index\.html"
```

(This would match index.html, index.html?user=pv, or anything else that a client might want to append) A much safer rule would be to define the number of characters that may follow. The following allows 0-64 characters to follow:

```
EAccessRule permit "^GET /index\.html.{0,64}$"
```

Quite often, companies monitor the availability of their website using tools that make requests using the HEAD command. We could add this as a separate entry:

```
EAccessRule permit "^HEAD /index\.html$"
```

Or these two rules can be consolidated into:

```
EAccessRule permit "^(GET|HEAD) /index\.html$"
```

Appendix B: Protecting an Exchange 5.5 server running OWA (Outlook Web Access).

As a final example, The following process was used to create the Eaccess rules to protect an exchange 5.5 server running OWA. The resulting rule set demonstrates the power of regular expressions in mod_eaccess.

First, we take the OWA log file in the following format

```
#Fields: date time c-ip cs-username cs-method cs-uri-stem cs-uri-query sc-status time-
taken cs(Cookie)
2001-10-18 01:06:31  test/pvinciguerra GET /exchange/USA/inbox/commands.asp
command=checkmessages&view=1&page=1&obj=00000000E865E4EDC8F3D3118B8100A0C9D176C10100CFF4
7904F265D3118B7300A0C9D176C10000002B7A3E0000&store=0 200 375
ASPSESSIONIDQGQGGRSR=HDINHACCFHCCBKNNMMKHHDND
2001-10-18 01:06:31 192.168.1.1 test/pvinciguerra GET /exchange/USA/logon.asp
newwindow=1&viewer=1 200 0 ASPSESSIONIDQGQGGRSR=HDINHACCFHCCBKNNMMKHHDND
2001-10-18 01:06:42 192.168.1.1 test/pvinciguerra GET /exchange/USA/LogonFrm.asp
isnewwindow=1&mailbox=pvinciguerra 401 0 ASPSESSIONIDQGQGGRSR=HDINHACCFHCCBKNNMMKHHDND
```

We then use the following script to generate the eaccess rule set. This script takes each of our allowed urls as before and searches for it in our log file. It the prints the eaccess rule in the proper format. The rule it then passed through sed which will do replacements based upon rules I have created in a file called sed-file. Sort and uniq provide a single instance of the rule. Finally, the rule needs to be cleaned up by stripping off the trailing "?-" which appears when there is no query string.

eaccess.sh

```
#!/bin/sh
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
cat urls.uniq | while read i

   do

     echo ' ';
     (grep "$i" ex011018.log|awk -F" " '{print "EAccessRule permit \"^"$5 " "$6 "?"
$7"$\"" }';) |sed -f sed-file |sort|uniq|sed -e 's/?-//g'
done
```

By looking at the output of the eaccess.sh script and identifying the character patterns, we can create the sed-file.

One rule:

```
EAccessRule permit ^GET
/exchange/USA/inbox/commands.asp?command=checkmessages&view=1&page=1&obj=00000000E
865E4EDC8F3D3118B8100A0C9D176C10100CFF47904F265D3118B7300A0C9D176C10000002B7A3E000
0&store=0
```

By visual inspection the object token is a 92 character hexadecimal number. This can be represented by "obj=[0-9A-F]{92}". Within the sed-file, we can match the 92 character hex number and replace it with the representative regex. Through the process of stepwise refinement, we come to our final set of eaccess rules based upon the following sed-file.

sed-file

```
s/obj=[0-9A-F]\{220\}/obj=[0-9A-F]{220}/g
s/obj=[0-9A-F]\{140\}/obj=[0-9A-F]{140}/g
s/obj=[0-9A-F]\{92\}/obj=[0-9A-F]{92}/g
s/obj=[0-9A-F]\{64\}/obj=[0-9A-F]{64}/g
s/obj=[0-9]\{1,5\}/obj=[0-9]{1,5}/g
s/page=[0-9]\{1,3\}/page=[0-9]{1,3}/g
s/view=[0-9]/view=[0-9]/g
s/store=[012]/store=[012]/g
s/compidx=[012]/compidx=[012]/g
s/index=[0-9]\{1,3\}/index=[0-9]{1,3}/g
s/command=\(delete\|forward\|reply\|replyall\)/command=(delete|forward|reply|rep
lyall)/g
s/item\.asp\?action=\(next\|prev\)/item.asp?action=(next|prev)/g
s/IsSavedRegAppt=\([Ff]alse\|True\)/IsSavedRegAppt=([Ff]alse|True)/g
s/imp=[12]/imp=[12]/g
s/type=[017]/type=[017]/g
s/msgtype=[017]/msgtype=[017]/g
s/tab=[12]/tab=[12]/g
s/att=[01]/att=[01]/g
s/mailbox=[a-zA-Z0-9]\{1,25\}/mailbox=[a-zA-Z0-9]{1,25}/g
s/inbox\/commands.asp?command=\(deleteallmessages\|deletefolder\|checkmessages\|
newfolder\|nothing\|updateview\)/inbox\/commands.asp?command=(deleteallmessages|
deletefolder|checkmessages|newfolder|nothing|updateview)/g
s/inbox\/commands.asp?action=\(deleteallmessages\|deletefolder\)/inbox\/commands
.asp?action=(deleteallmessages|deletefolder)/g
s/att=ATT\-[01]\-[0-9A-F]\{32\}\-.\{0,255\}\$/att=ATT-[01]-[0-9A-F]{32}-.{0,255}
$/g
s/objID=[0-9]\{4,6\}/objID=[0-9]{4,6}/g
s/LogonFrm\.asp\?isnewwindow=[01]/LogonFrm\.asp\?isnewwindow=[01]/g
s/M=[0-9]\{1,2\}/M=[0-9]{1,2}/g
s/D=[0-9]\{1,2\}/D=[0-9]{1,2}/g
s/Y=[12][0-9]\{3\}/Y=[12][0-9]{3}/g
s/ffname=.\{1,255\}&/ffname=.{1,255}\&/g
```

conf/eaccess_acls

```
EAccessRule permit "^GET /exchange/USA/Attach/generic.gif$"

EAccessRule permit "^GET /exchange/USA/Attach/read.asp?obj=[0-9A-F]{140}&att=ATT-[01]-
[0-9A-F]{32}-.{0,255}$"

EAccessRule permit "^GET /exchange/USA/Default.htm$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
EAccessRule permit "^GET /exchange/USA/Forms/IPM/NOTE/cmpAtt.ASP?ffname=.{1,255}&$"

EAccessRule permit "^GET /exchange/USA/Forms/IPM/NOTE/commands.asp$"

EAccessRule permit "^GET /exchange/USA/LogonFrm.asp?isnewwindow=0&mailbox=[a-zA-Z0-
9]{1,25}$"
EAccessRule permit "^GET /exchange/USA/LogonFrm.asp?isnewwindow=0&mailbox=[a-zA-Z0-
9]{1,25}+$"
EAccessRule permit "^GET /exchange/USA/LogonFrm.asp?isnewwindow=1&mailbox=[a-zA-Z0-
9]{1,25}$"

EAccessRule permit "^GET /exchange/USA/Navbar/cal.gif$"

EAccessRule permit "^GET /exchange/USA/Navbar/contact.gif$"

EAccessRule permit "^GET /exchange/USA/Navbar/finduser.gif$"

EAccessRule permit "^GET /exchange/USA/Navbar/inbox.gif$"

EAccessRule permit "^GET /exchange/USA/Navbar/logoff.gif$"

EAccessRule permit "^GET /exchange/USA/Navbar/nbInbox.asp$"

EAccessRule permit "^GET /exchange/USA/Navbar/option.gif$"

EAccessRule permit "^GET /exchange/USA/Navbar/public.gif$"

EAccessRule permit "^GET /exchange/USA/back.jpg$"

EAccessRule permit "^GET /exchange/USA/calendar/Calendar.class$"

EAccessRule permit "^GET /exchange/USA/calendar/DateNavigator.class$"

EAccessRule permit "^GET /exchange/USA/calendar/DateNavigatorSelection.class$"

EAccessRule permit "^GET /exchange/USA/calendar/Global.class$"

EAccessRule permit "^GET /exchange/USA/calendar/GotoDate.class$"

EAccessRule permit "^GET /exchange/USA/calendar/MsgBox.class$"

EAccessRule permit "^GET /exchange/USA/calendar/SuperDate.class$"

EAccessRule permit "^GET /exchange/USA/calendar/appts.asp?M=[0-9]{1,2}&D=[0-
9]{1,2}&Y=[12][0-9]{3}&view=[0-9]$"
EAccessRule permit "^GET /exchange/USA/calendar/appts.asp?view=[0-9]&session=1$"

EAccessRule permit "^GET /exchange/USA/calendar/events.asp?M=[0-9]{1,2}&D=[0-
9]{1,2}&Y=[12][0-9]{3}&view=[0-9]$"
EAccessRule permit "^GET /exchange/USA/calendar/events.asp?view=[0-
9]&session=1&caller=main_fr$"

EAccessRule permit "^GET /exchange/USA/calendar/main_fr.asp$"
EAccessRule permit "^GET /exchange/USA/calendar/main_fr.asp?store=[012]&obj=[0-9A-
F]{92}$"
EAccessRule permit "^GET /exchange/USA/calendar/main_fr.asp?view=[0-9]&obj=[0-9A-
F]{92}$"

EAccessRule permit "^GET /exchange/USA/calendar/pick.asp?view=[0-9]&session=1$"

EAccessRule permit "^GET /exchange/USA/calendar/title.asp?view=[0-9]&session=1&obj=$"
EAccessRule permit "^GET /exchange/USA/calendar/title.asp?view=[0-9]&session=1&obj=[0-
9A-F]{92}$"

EAccessRule permit "^GET
/exchange/USA/contacts/commands.asp?command=checkmessages&view=[0-9]&page=[0-
9]{1,3}&obj=[0-9A-]{92}&store=[012]$"
EAccessRule permit "^GET
/exchange/USA/contacts/commands.asp?command=nothing&store=[012]$"

EAccessRule permit "^GET /exchange/USA/contacts/main_fr.asp?store=[012]&obj=[0-9A-
F]{92}$"

EAccessRule permit "^GET /exchange/USA/contacts/messages.asp?obj=[0-9A-
F]{92}&store=[012]$"

EAccessRule permit "^GET /exchange/USA/contacts/peerfldr.asp?obj=[0-9A-
F]{92}&store=[012]$"

EAccessRule permit "^GET /exchange/USA/contacts/title.asp?compidx=[012]&store=[012]$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
EAccessRule permit "^GET /exchange/USA/contacts/title.asp?obj=[0-9A-
F]{92}&acs=&compidx=[012]&store=[012]$"

EAccessRule permit "^GET /exchange/USA/finduser/details.asp?obj=[0-9A-F]{64}$"

EAccessRule permit "^GET /exchange/USA/finduser/fumid.asp$"

EAccessRule permit "^GET /exchange/USA/finduser/fumsgdef.asp$"

EAccessRule permit "^GET /exchange/USA/finduser/root.asp$"

EAccessRule permit "^GET /exchange/USA/forms/Delete.GIF$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/CONTACT/commands.asp?obj=[0-9A-
F]{140}$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/CONTACT/frmRoot.asp?index=[0-
9]{1,3}&obj=[0-9A-F]{140}&command=open$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/CONTACT/frmroot.asp?obj=[0-9A-
F]{140}&command=open$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/CONTACT/postMsg.asp?new=False&obj=[0-
9A-F]{140}$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/CONTACT/postTitl.asp?obj=[0-9A-
F]{140}&command=open&tab=[12]&att=[01]&imp=[12]$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/cmpMsg.asp?obj=[0-
9]{1,5}&caller=1$"

EAccessRule permit "^GET
/exchange/USA/forms/IPM/NOTE/cmpTitle.asp?tab=[12]&att=[01]&imp=[12]$"

EAccessRule permit "^GET
/exchange/USA/forms/IPM/NOTE/commands.asp?command=(delete|forward|reply|replyall)&obj=[0
-9A-F]{140}$"
EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/commands.asp?obj=[0-9]{1,5}$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/frmRoot.asp?command=new&obj=[0-
9]{1,5}$"
EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/frmRoot.asp?index=[0-
9]{1,3}&obj=[0-9A-F]{140}&command=open$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/frmroot.asp?obj=[0-9A-
F]{140}&command=open$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/icon.jpg$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/m16spacer.gif$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/read.asp?command=open&obj=[0-9A-
F]{140}&timedout=$"

EAccessRule permit "^GET
/exchange/USA/forms/IPM/SCHEDULE/MEETING/REQUEST/commands.asp?command=open&obj=[0-9A-
F]{140}&msgtype=[017]$"

EAccessRule permit "^GET
/exchange/USA/forms/IPM/SCHEDULE/MEETING/REQUEST/frmRoot.asp?index=[0-9]{1,3}&obj=[0-9A-
F]{140}&command=open$"

EAccessRule permit "^GET
/exchange/USA/forms/IPM/SCHEDULE/MEETING/REQUEST/mrread.asp?command=open&obj=[0-9A-
F]{140}&CurrUserIsOrg=False$"

EAccessRule permit "^GET /exchange/USA/forms/LOWDOWN.gif$"

EAccessRule permit "^GET /exchange/USA/forms/ReplyFld.gif$"

EAccessRule permit "^GET
/exchange/USA/forms/amunres.asp?att=[01]&type=[017]&imp=[12]&IsSavedRegAppt=([Ff]alse|Tr
ue)&tab=[12]57&rtn=r&obj=[0-9]{1,5}&cc=0$"
EAccessRule permit "^GET /exchange/USA/forms/amunres.asp?tab=[12]57&obj=[0-
9]{1,5}&cc=1&rtn=m&bcc=0$"

EAccessRule permit "^GET /exchange/USA/forms/caninvit.gif$"

EAccessRule permit "^GET /exchange/USA/forms/copynew.asp$"

EAccessRule permit "^GET /exchange/USA/forms/copynew.gif$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
EAccessRule permit "^GET /exchange/USA/forms/delmark.gif$"

EAccessRule permit "^GET /exchange/USA/forms/delrecur.gif$"

EAccessRule permit "^GET /exchange/USA/forms/edseries.gif$"

EAccessRule permit "^GET /exchange/USA/forms/explore.gif$"

EAccessRule permit "^GET /exchange/USA/forms/forward.gif$"

EAccessRule permit "^GET /exchange/USA/forms/high.gif$"

EAccessRule permit "^GET /exchange/USA/forms/highdown.gif$"

EAccessRule permit "^GET /exchange/USA/forms/inviteat.gif$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/contact/commands.asp?command=cancel&obj=[0-9A-F]{140}$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/contact/commands.asp?command=cancel&obj=[0-9]{1,5}$"
EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/commands.asp?obj=[0-9]{1,5}$"

EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/contdet.asp?obj=[0-9A-F]{140}$"
EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/contdet.asp?obj=[0-9]{1,5}$"

EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/frmroot.asp?command=new$"

EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/postAtt.asp?obj=[0-9A-F]{140}$"
EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/postAtt.asp?obj=[0-9]{1,5}$"

EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/postMsg.asp?new=1&obj=[0-
9]{1,5}$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/contact/postTitl.asp?command=new&tab=[12]&att=[01]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/contact/postTitl.asp?command=open&tab=[12]&att=[01]$"
EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/postTitl.asp?obj=[0-
9]{1,5}&command=new&tab=[12]&att=&imp=[12]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/contact/postTitl.asp?tab=3&command=new&att=[01]&imp=undefined$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/contact/postTitl.asp?tab=3&command=open&att=[01]&imp=undefined$"

EAccessRule permit "^GET /exchange/USA/forms/ipm/note/cmpAtt.asp?obj=[0-9]{1,5}$
"

EAccessRule permit "^GET /exchange/USA/forms/ipm/note/cmpMsg.asp?obj=[0-
9]{1,5}&caller=1$"
EAccessRule permit "^GET /exchange/USA/forms/ipm/note/cmpMsg.asp?obj=[0-
9]{1,5}&cc=1&bcc=0$"

EAccessRule permit "^GET /exchange/USA/forms/ipm/note/cmpTitle.asp?obj=[0-
9]{1,5}&tab=[12]&att=[01]&imp=[12]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/note/cmpTitle.asp?tab=[12]&att=[01]&imp=[12]$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/note/cmptitle.asp?tab=[12]&att=[01]&imp=0$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/note/cmptitle.asp?tab=[12]&att=[01]&imp=[12]$"

EAccessRule permit "^GET /exchange/USA/forms/ipm/note/commands.asp?command=send&obj=[0-
9]{1,5}&saveCopy=true&imp=[12]$"
EAccessRule permit "^GET /exchange/USA/forms/ipm/note/commands.asp?obj=[0-9]{1,5}$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/note/frmroot.asp?command=new&store=[012]$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/commands.asp?command=editrecur&obj=[0-
9A-F]{220}$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/commands.asp?command=editseries&obj=[0-
9A-F]{220}&msgtype=[017]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/commands.asp?command=new&obj=[0-
9]{1,5}&msgtype=[017]$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/commands.asp?command=read&obj=[0-9A-
F]{220}&msgtype=[017]$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/frmRoot.asp?command=read&obj=[0-9A-
F]{220}$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/frmRoot.asp?obj=[0-9A-
F]{220}&command=editseries$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/frmroot.asp?command=new&type=[017]$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrAppt.asp?command=new&obj=[0-
9]{1,5}&type=[017]&cc=0$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrAppt.asp?obj=[0-9A-
F]{220}&command=editseries&root=1&type=[017]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrAppt.asp?obj=[0-9A-
F]{220}&command=read&root=1&type=[017]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrAppt.asp?obj=[0-
9]{1,5}&command=new&root=1&type=[017]$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrAtt.asp?obj=[0-
9]{1,5}&cc=0&IsSavedRegAppt=([Ff]alse|True)$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrOpt.asp?command=new&obj=[0-
9]{1,5}&sc=true&cc=0$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrPlaner.asp?command=new&obj=[0-
9]{1,5}&type=[017]&cc=0$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrRecur.asp?command=new&obj=[0-
9]{1,5}&cc=0$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?command=new&obj=[0-
9]{1,5}&tab=3&att=[01]&type=[017]&imp=[12]&IsSavedRegAppt=([Ff]alse|True)$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?command=new&obj=[0-
9]{1,5}&tab=5&att=[01]&type=[017]&imp=[12]&IsSavedRegAppt=([Ff]alse|True)$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?command=new&obj=[0-
9]{1,5}&tab=[12]&att=[01]&type=[017]&IsSavedRegAppt=([Ff]alse|True)$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?command=new&obj=[0-
9]{1,5}&tab=[12]&att=[01]&type=[017]&imp=[12]&IsSavedRegAppt=([Ff]alse|True)$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?command=new&obj=[0-
9]{1,5}&tab=[12]57&att=[01]&type=[017]&imp=[12]&IsSavedRegAppt=([Ff]alse|True)$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?obj=[0-9A-
F]{220}&command=editseries&tab=[12]&att=[01]&imp=0&type=[017]&IsSavedRegAppt=([Ff]alse|T
rue)$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?obj=[0-9A-
F]{220}&command=read&tab=[12]&att=[01]&imp=0&type=[017]&IsSavedRegAppt=([Ff]alse|True)$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?obj=[0-9A-
F]{220}&command=read&tab=[12]&att=[01]&imp=[12]&type=[017]&IsSavedRegAppt=([Ff]alse|True
)$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?obj=[0-
9]{1,5}&command=new&tab=4&att=[01]&IsSavedRegAppt=([Ff]alse|True)&imp=[12]&type=[017]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?obj=[0-
9]{1,5}&command=new&tab=[12]&att=[01]&imp=[12]&type=[017]&IsSavedRegAppt=([Ff]alse|True)
$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrtitle.asp?command=editseries&obj=[0-
9A-F]{220}&tab=[12]&att=[01]&type=[017]&IsSavedRegAppt=([Ff]alse|True)&imp=[12]$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrtitle.asp?command=read&obj=[0-9A-
F]{220}&tab=[12]&att=[01]&type=[017]&IsSavedRegAppt=([Ff]alse|True)&imp=0$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrtitle.asp?command=read&obj=[0-9A-
F]{220}&tab=[12]&att=[01]&type=[017]&IsSavedRegAppt=([Ff]alse|True)&imp=[12]$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/resp/commands.asp?obj=[0-9]{1,5}$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/resp/frmRoot.asp?obj=[0-
9]{1,5}&cancelMR=2&replyMR=0$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/resp/rspMsg.asp?obj=[0-
9]{1,5}&caller=1&milTime=0&replyMR=0&replyCancel=0$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/resp/rspTitle.asp?tab=[12]&att=[01]&imp=[12]&ms
gType=0&cancelMR=2$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/resp/rsptitle.asp?tab=[12]&att=[01]&imp=[12]&ms
gType=0&cancelMR=2$"

EAccessRule permit "^GET /exchange/USA/forms/low.gif$"

EAccessRule permit "^GET /exchange/USA/forms/mailcont.gif$"

EAccessRule permit "^GET /exchange/USA/forms/movcpy.gif$"

EAccessRule permit "^GET /exchange/USA/forms/mtgaccpt.gif$"

EAccessRule permit "^GET /exchange/USA/forms/mtgcont.gif$"

EAccessRule permit "^GET /exchange/USA/forms/mtgdecln.gif$"

EAccessRule permit "^GET /exchange/USA/forms/mtgtent.gif$"

EAccessRule permit "^GET /exchange/USA/forms/nextmsg.gif$"

EAccessRule permit "^GET /exchange/USA/forms/prevmsg.gif$"

EAccessRule permit "^GET /exchange/USA/forms/reply.gif$"

EAccessRule permit "^GET /exchange/USA/forms/replyall.gif$"

EAccessRule permit "^GET /exchange/USA/forms/resolve.gif$"

EAccessRule permit "^GET /exchange/USA/forms/save.gif$"

EAccessRule permit "^GET /exchange/USA/forms/send.gif$"

EAccessRule permit "^GET /exchange/USA/forms/showmap.gif$"

EAccessRule permit "^GET /exchange/USA/forms/tabWdot.gif$"

EAccessRule permit "^GET /exchange/USA/forms/tablcor.gif$"

EAccessRule permit "^GET /exchange/USA/forms/tabrcor.gif$"

EAccessRule permit "^GET /exchange/USA/forms/tabrline.gif$"

EAccessRule permit "^GET /exchange/USA/forms/viewcal.gif$"

EAccessRule permit "^GET /exchange/USA/help/calcalar.gif$"

EAccessRule permit "^GET /exchange/USA/help/calfrm.gif$"

EAccessRule permit "^GET /exchange/USA/help/calhelp.gif$"

EAccessRule permit "^GET /exchange/USA/help/calnavbr.gif$"

EAccessRule permit "^GET /exchange/USA/help/calover.htm$"

EAccessRule permit "^GET /exchange/USA/help/calscdar.gif$"

EAccessRule permit "^GET /exchange/USA/images/arwtanlf.gif$"

EAccessRule permit "^GET /exchange/USA/images/arwtanrt.gif$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
EAccessRule permit "^GET /exchange/USA/images/calendar.gif$"
EAccessRule permit "^GET /exchange/USA/images/contact.gif$"
EAccessRule permit "^GET /exchange/USA/images/deleted.gif$"
EAccessRule permit "^GET /exchange/USA/images/delfoldr.gif$"
EAccessRule permit "^GET /exchange/USA/images/delmsg.gif$"
EAccessRule permit "^GET /exchange/USA/images/divider.gif$"
EAccessRule permit "^GET /exchange/USA/images/empfldr.gif$"
EAccessRule permit "^GET /exchange/USA/images/envelope.gif$"
EAccessRule permit "^GET /exchange/USA/images/folder.gif$"
EAccessRule permit "^GET /exchange/USA/images/help.gif$"
EAccessRule permit "^GET /exchange/USA/images/inbox.gif$"
EAccessRule permit "^GET /exchange/USA/images/low.gif$"
EAccessRule permit "^GET /exchange/USA/images/mailbox.gif$"
EAccessRule permit "^GET /exchange/USA/images/mark.gif$"
EAccessRule permit "^GET /exchange/USA/images/meeting.gif$"
EAccessRule permit "^GET /exchange/USA/images/mffav.gif$"
EAccessRule permit "^GET /exchange/USA/images/movcpy.gif$"
EAccessRule permit "^GET /exchange/USA/images/mtgcancl.gif$"
EAccessRule permit "^GET /exchange/USA/images/mtgreq.gif$"
EAccessRule permit "^GET /exchange/USA/images/ndr.gif$"
EAccessRule permit "^GET /exchange/USA/images/newappt.gif$"
EAccessRule permit "^GET /exchange/USA/images/newcont.gif$"
EAccessRule permit "^GET /exchange/USA/images/newfoldr.gif$"
EAccessRule permit "^GET /exchange/USA/images/newmail.gif$"
EAccessRule permit "^GET /exchange/USA/images/newmtg.gif$"
EAccessRule permit "^GET /exchange/USA/images/newpost.gif$"
EAccessRule permit "^GET /exchange/USA/images/outbox.gif$"
EAccessRule permit "^GET /exchange/USA/images/papclip.gif$"
EAccessRule permit "^GET /exchange/USA/images/prop.gif$"
EAccessRule permit "^GET /exchange/USA/images/recur.gif$"
EAccessRule permit "^GET /exchange/USA/images/refresh.gif$"
EAccessRule permit "^GET /exchange/USA/images/sent_itm.gif$"
EAccessRule permit "^GET /exchange/USA/images/upone.gif$"
EAccessRule permit "^GET /exchange/USA/images/urgent.gif$"


EAccessRule permit "^GET
/exchange/USA/inbox/commands.asp?action=(deleteallmessages|deletefolder)&obj=[0-9A-
F]{92}&store=[012]$"
EAccessRule permit "^GET
/exchange/USA/inbox/commands.asp?command=(deleteallmessages|deletefolder|checkmessages|n
ewfolder|nothing|updateview)&obj=[0-9A-F]{92}&s
tore=[012]$"
EAccessRule permit "^GET
/exchange/USA/inbox/commands.asp?command=(deleteallmessages|deletefolder|checkmessages|n
ewfolder|nothing|updateview)&store=[012]$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
EAccessRule permit "^GET
/exchange/USA/inbox/commands.asp?command=(deleteallmessages|deletefolder|checkmessages|n
ewfolder|nothing|updateview)&view=[0-9]&page=[0
-9]{1,3}&obj=[0-9A-F]{92}&store=[012]$"
EAccessRule permit "^GET
/exchange/USA/inbox/commands.asp?store=[012]&command=newfolder$"

EAccessRule permit "^GET /exchange/USA/inbox/envelope.gif$"

EAccessRule permit "^GET
/exchange/USA/inbox/main_fr.asp?store=[012]&command=newfolder&obj=[0-9A-F]{92}$"
EAccessRule permit "^GET /exchange/USA/inbox/main_fr.asp?store=[012]&obj=$"
EAccessRule permit "^GET /exchange/USA/inbox/main_fr.asp?view=[0-
9]&store=[012]&obj=&acs=$"

EAccessRule permit "^GET /exchange/USA/inbox/messages.asp?obj=[0-9A-F]{92}&page=[0-
9]{1,3}$"
EAccessRule permit "^GET /exchange/USA/inbox/messages.asp?obj=[0-9A-F]{92}&page=[0-
9]{1,3}&view=[0-9]&compidx=[012]&store=[012]$"
EAccessRule permit "^GET /exchange/USA/inbox/messages.asp?obj=[0-9A-F]{92}&store=[012]$"

EAccessRule permit "^GET /exchange/USA/inbox/papclip.gif$"

EAccessRule permit "^GET /exchange/USA/inbox/peerfldr.asp?obj=[0-9A-F]{92}&store=[012]$"
EAccessRule permit "^GET /exchange/USA/inbox/peerfldr.asp?obj=[0-9A-
F]{92}&store=[012]&timedout=false$"

EAccessRule permit "^GET /exchange/USA/inbox/title.asp?compidx=[012]&store=[012]$"
EAccessRule permit "^GET /exchange/USA/inbox/title.asp?obj=[0-9A-
F]{92}&acs=&compidx=[012]&store=[012]$"
EAccessRule permit "^GET /exchange/USA/inbox/title.asp?page=[0-9]{1,3}&view=[0-
9]&compidx=[012]$"

EAccessRule permit "^GET /exchange/USA/inbox/urgent.gif$"

EAccessRule permit "^GET /exchange/USA/item.asp?action=next$"
EAccessRule permit "^GET /exchange/USA/item.asp?action=prev$"

EAccessRule permit "^GET /exchange/USA/logoff.asp$"

EAccessRule permit "^GET /exchange/USA/logon.asp$"
EAccessRule permit "^GET /exchange/USA/logon.asp?newwindow=1&viewer=1$"

EAccessRule permit "^GET /exchange/USA/msie.gif$"

EAccessRule permit "^GET /exchange/USA/msprod.gif$"

EAccessRule permit "^GET /exchange/USA/options/set.asp$"

EAccessRule permit "^GET /exchange/USA/part1.gif$"

EAccessRule permit "^GET /exchange/USA/part2.gif$"

EAccessRule permit "^GET /exchange/USA/relogon.htm$"

EAccessRule permit "^GET /exchange/USA/root.asp$"
EAccessRule permit "^GET /exchange/USA/root.asp?view=[0-9]&store=[012]&obj=$"
EAccessRule permit "^GET /exchange/USA/root.asp?view=[0-9]&store=[012]&obj=[0-9A-
F]{92}$"

EAccessRule permit "^POST
/exchange/USA/contacts/commands.asp?action=deletemarkedmessages$"

EAccessRule permit "^POST /exchange/USA/finduser/fumsg.asp$"

EAccessRule permit "^POST /exchange/USA/forms/IPM/CONTACT/commands.asp$"

EAccessRule permit "^POST /exchange/USA/forms/IPM/NOTE/commands.asp$"

EAccessRule permit "^POST /exchange/USA/forms/ipm/contact/commands.asp$"

EAccessRule permit "^POST /exchange/USA/forms/ipm/note/commands.asp$"
EAccessRule permit "^POST /exchange/USA/forms/ipm/note/commands.asp?tab=[12]57&obj=[0-
9]{1,5}&cc=1&rtn=m&bcc=0$"

EAccessRule permit "^POST
/exchange/USA/forms/ipm/schedule/meeting/request/commands.asp$"
EAccessRule permit "^POST
/exchange/USA/forms/ipm/schedule/meeting/request/commands.asp?att=[01]&type=[017]&imp=[1
2]&IsSavedRegAppt=([Ff]alse|True)&tab=[12]57&r
tn=r&obj=[0-9]{1,5}&cc=0$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
EAccessRule permit "^POST /exchange/USA/forms/ipm/schedule/meeting/resp/commands.asp$"

EAccessRule permit "^POST /exchange/USA/inbox/commands.asp$"
EAccessRule permit "^POST /exchange/USA/inbox/commands.asp?action=deletemarkedmessages$"

EAccessRule permit "^POST /exchange/USA/options/set.asp$"

EAccessRule permit "^POST /exchange/exupload.dll$"
[pvinci@whatbox exchange]$ cat eaccess_acl

EAccessRule permit "^GET /exchange/USA/Attach/generic.gif$"

EAccessRule permit "^GET /exchange/USA/Attach/read.asp?obj=[0-9A-F]{140}&att=ATT-[01]-
[0-9A-F]{32}-.{0,255}$"

EAccessRule permit "^GET /exchange/USA/Default.htm$"

EAccessRule permit "^GET /exchange/USA/Forms/IPM/NOTE/cmpAtt.ASP?ffname=.{1,255}&$"

EAccessRule permit "^GET /exchange/USA/Forms/IPM/NOTE/commands.asp$"

EAccessRule permit "^GET /exchange/USA/LogonFrm.asp?isnewwindow=0&mailbox=[a-zA-Z0-
9]{1,25}$"
EAccessRule permit "^GET /exchange/USA/LogonFrm.asp?isnewwindow=0&mailbox=[a-zA-Z0-
9]{1,25}+$"
EAccessRule permit "^GET /exchange/USA/LogonFrm.asp?isnewwindow=1&mailbox=[a-zA-Z0-
9]{1,25}$"

EAccessRule permit "^GET /exchange/USA/Navbar/cal.gif$"

EAccessRule permit "^GET /exchange/USA/Navbar/contact.gif$"

EAccessRule permit "^GET /exchange/USA/Navbar/finduser.gif$"

EAccessRule permit "^GET /exchange/USA/Navbar/inbox.gif$"

EAccessRule permit "^GET /exchange/USA/Navbar/logoff.gif$"

EAccessRule permit "^GET /exchange/USA/Navbar/nbInbox.asp$"

EAccessRule permit "^GET /exchange/USA/Navbar/option.gif$"

EAccessRule permit "^GET /exchange/USA/Navbar/public.gif$"

EAccessRule permit "^GET /exchange/USA/back.jpg$"

EAccessRule permit "^GET /exchange/USA/calendar/Calendar.class$"

EAccessRule permit "^GET /exchange/USA/calendar/DateNavigator.class$"

EAccessRule permit "^GET /exchange/USA/calendar/DateNavigatorSelection.class$"

EAccessRule permit "^GET /exchange/USA/calendar/Global.class$"

EAccessRule permit "^GET /exchange/USA/calendar/GotoDate.class$"

EAccessRule permit "^GET /exchange/USA/calendar/MsgBox.class$"

EAccessRule permit "^GET /exchange/USA/calendar/SuperDate.class$"

EAccessRule permit "^GET /exchange/USA/calendar/appts.asp?M=[0-9]{1,2}&D=[0-
9]{1,2}&Y=[12][0-9]{3}&view=[0-9]$"
EAccessRule permit "^GET /exchange/USA/calendar/appts.asp?view=[0-9]&session=1$"

EAccessRule permit "^GET /exchange/USA/calendar/events.asp?M=[0-9]{1,2}&D=[0-
9]{1,2}&Y=[12][0-9]{3}&view=[0-9]$"
EAccessRule permit "^GET /exchange/USA/calendar/events.asp?view=[0-
9]&session=1&caller=main_fr$"

EAccessRule permit "^GET /exchange/USA/calendar/main_fr.asp$"
EAccessRule permit "^GET /exchange/USA/calendar/main_fr.asp?store=[012]&obj=[0-9A-
F]{92}$"
EAccessRule permit "^GET /exchange/USA/calendar/main_fr.asp?view=[0-9]&obj=[0-9A-
F]{92}$"

EAccessRule permit "^GET /exchange/USA/calendar/pick.asp?view=[0-9]&session=1$"

EAccessRule permit "^GET /exchange/USA/calendar/title.asp?view=[0-9]&session=1&obj=$"
EAccessRule permit "^GET /exchange/USA/calendar/title.asp?view=[0-9]&session=1&obj=[0-
9A-F]{92}$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
EAccessRule permit "^GET
/exchange/USA/contacts/commands.asp?command=checkmessages&view=[0-9]&page=[0-
9]{1,3}&obj=[0-9A-F]{92}&store=[012]$"
EAccessRule permit "^GET
/exchange/USA/contacts/commands.asp?command=nothing&store=[012]$"

EAccessRule permit "^GET /exchange/USA/contacts/main_fr.asp?store=[012]&obj=[0-9A-
F]{92}$"

EAccessRule permit "^GET /exchange/USA/contacts/messages.asp?obj=[0-9A-
F]{92}&store=[012]$"

EAccessRule permit "^GET /exchange/USA/contacts/peerfldr.asp?obj=[0-9A-
F]{92}&store=[012]$"

EAccessRule permit "^GET /exchange/USA/contacts/title.asp?compidx=[012]&store=[012]$"
EAccessRule permit "^GET /exchange/USA/contacts/title.asp?obj=[0-9A-
F]{92}&acs=&compidx=[012]&store=[012]$"

EAccessRule permit "^GET /exchange/USA/finduser/details.asp?obj=[0-9A-F]{64}$"

EAccessRule permit "^GET /exchange/USA/finduser/fumid.asp$"

EAccessRule permit "^GET /exchange/USA/finduser/fumsgdef.asp$"

EAccessRule permit "^GET /exchange/USA/finduser/root.asp$"

EAccessRule permit "^GET /exchange/USA/forms/Delete.GIF$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/CONTACT/commands.asp?obj=[0-9A-
F]{140}$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/CONTACT/frmRoot.asp?index=[0-
9]{1,3}&obj=[0-9A-F]{140}&command=open$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/CONTACT/frmroot.asp?obj=[0-9A-
F]{140}&command=open$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/CONTACT/postMsg.asp?new=False&obj=[0-
9A-F]{140}$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/CONTACT/postTitl.asp?obj=[0-9A-
F]{140}&command=open&tab=[12]&att=[01]&imp=[12]$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/cmpMsg.asp?obj=[0-
9]{1,5}&caller=1$"

EAccessRule permit "^GET
/exchange/USA/forms/IPM/NOTE/cmpTitle.asp?tab=[12]&att=[01]&imp=[12]$"

EAccessRule permit "^GET
/exchange/USA/forms/IPM/NOTE/commands.asp?command=(delete|forward|reply|replyall)&obj=[0
-9A-F]{140}$"
EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/commands.asp?obj=[0-9]{1,5}$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/frmRoot.asp?command=new&obj=[0-
9]{1,5}$"
EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/frmRoot.asp?index=[0-
9]{1,3}&obj=[0-9A-F]{140}&command=open$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/frmroot.asp?obj=[0-9A-
F]{140}&command=open$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/icon.jpg$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/m16spacer.gif$"

EAccessRule permit "^GET /exchange/USA/forms/IPM/NOTE/read.asp?command=open&obj=[0-9A-
F]{140}&timedout=$"

EAccessRule permit "^GET
/exchange/USA/forms/IPM/SCHEDULE/MEETING/REQUEST/commands.asp?command=open&obj=[0-9A-
F]{140}&msgtype=[017]$"

EAccessRule permit "^GET
/exchange/USA/forms/IPM/SCHEDULE/MEETING/REQUEST/frmRoot.asp?index=[0-9]{1,3}&obj=[0-9A-
F]{140}&command=open$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
EAccessRule permit "^GET
/exchange/USA/forms/IPM/SCHEDULE/MEETING/REQUEST/mrread.asp?command=open&obj=[0-9A-
F]{140}&CurrUserIsOrg=False$"

EAccessRule permit "^GET /exchange/USA/forms/LOWDOWN.gif$"

EAccessRule permit "^GET /exchange/USA/forms/ReplyFld.gif$"

EAccessRule permit "^GET
/exchange/USA/forms/amunres.asp?att=[01]&type=[017]&imp=[12]&IsSavedRegAppt=([Ff]alse|Tr
ue)&tab=[12]57&rtn=r&obj=[0-9]{1,5}&cc=0$"
EAccessRule permit "^GET /exchange/USA/forms/amunres.asp?tab=[12]57&obj=[0-
9]{1,5}&cc=1&rtn=m&bcc=0$"

EAccessRule permit "^GET /exchange/USA/forms/caninvit.gif$"

EAccessRule permit "^GET /exchange/USA/forms/copynew.asp$"

EAccessRule permit "^GET /exchange/USA/forms/copynew.gif$"

EAccessRule permit "^GET /exchange/USA/forms/delmark.gif$"

EAccessRule permit "^GET /exchange/USA/forms/delrecur.gif$"

EAccessRule permit "^GET /exchange/USA/forms/edseries.gif$"

EAccessRule permit "^GET /exchange/USA/forms/explore.gif$"

EAccessRule permit "^GET /exchange/USA/forms/forward.gif$"

EAccessRule permit "^GET /exchange/USA/forms/high.gif$"

EAccessRule permit "^GET /exchange/USA/forms/highdown.gif$"

EAccessRule permit "^GET /exchange/USA/forms/inviteat.gif$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/contact/commands.asp?command=cancel&obj=[0-9A-F]{140}$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/contact/commands.asp?command=cancel&obj=[0-9]{1,5}$"
EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/commands.asp?obj=[0-9]{1,5}$"

EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/contdet.asp?obj=[0-9A-F]{140}$"
EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/contdet.asp?obj=[0-9]{1,5}$"

EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/frmroot.asp?command=new$"

EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/postAtt.asp?obj=[0-9A-F]{140}$"
EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/postAtt.asp?obj=[0-9]{1,5}$"

EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/postMsg.asp?new=1&obj=[0-
9]{1,5}$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/contact/postTitl.asp?command=new&tab=[12]&att=[01]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/contact/postTitl.asp?command=open&tab=[12]&att=[01]$"
EAccessRule permit "^GET /exchange/USA/forms/ipm/contact/postTitl.asp?obj=[0-
9]{1,5}&command=new&tab=[12]&att=&imp=[12]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/contact/postTitl.asp?tab=3&command=new&att=[01]&imp=undefined$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/contact/postTitl.asp?tab=3&command=open&att=[01]&imp=undefined$"

EAccessRule permit "^GET /exchange/USA/forms/ipm/note/cmpAtt.asp?obj=[0-9]{1,5}$
"

EAccessRule permit "^GET /exchange/USA/forms/ipm/note/cmpMsg.asp?obj=[0-
9]{1,5}&caller=1$"
EAccessRule permit "^GET /exchange/USA/forms/ipm/note/cmpMsg.asp?obj=[0-
9]{1,5}&cc=1&bcc=0$"

EAccessRule permit "^GET /exchange/USA/forms/ipm/note/cmpTitle.asp?obj=[0-
9]{1,5}&tab=[12]&att=[01]&imp=[12]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/note/cmpTitle.asp?tab=[12]&att=[01]&imp=[12]$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/note/cmptitle.asp?tab=[12]&att=[01]&imp=0$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/note/cmptitle.asp?tab=[12]&att=[01]&imp=[12]$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
EAccessRule permit "^GET /exchange/USA/forms/ipm/note/commands.asp?command=send&obj=[0-
9]{1,5}&saveCopy=true&imp=[12]$"
EAccessRule permit "^GET /exchange/USA/forms/ipm/note/commands.asp?obj=[0-9]{1,5}$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/note/frmroot.asp?command=new&store=[012]$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/commands.asp?command=editrecur&obj=[0-
9A-F]{220}$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/commands.asp?command=editseries&obj=[0-
9A-F]{220}&msgtype=[017]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/commands.asp?command=new&obj=[0-
9]{1,5}&msgtype=[017]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/commands.asp?command=read&obj=[0-9A-
F]{220}&msgtype=[017]$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/frmRoot.asp?command=read&obj=[0-9A-
F]{220}$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/frmRoot.asp?obj=[0-9A-
F]{220}&command=editseries$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/frmroot.asp?command=new&type=[017]$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrAppt.asp?command=new&obj=[0-
9]{1,5}&type=[017]&cc=0$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrAppt.asp?obj=[0-9A-
F]{220}&command=editseries&root=1&type=[017]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrAppt.asp?obj=[0-9A-
F]{220}&command=read&root=1&type=[017]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrAppt.asp?obj=[0-
9]{1,5}&command=new&root=1&type=[017]$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrAtt.asp?obj=[0-
9]{1,5}&cc=0&IsSavedRegAppt=([Ff]alse|True)$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrOpt.asp?command=new&obj=[0-
9]{1,5}&sc=true&cc=0$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrPlaner.asp?command=new&obj=[0-
9]{1,5}&type=[017]&cc=0$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrRecur.asp?command=new&obj=[0-
9]{1,5}&cc=0$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?command=new&obj=[0-
9]{1,5}&tab=3&att=[01]&type=[017]&imp=[12]&IsSavedRegAppt=([Ff]alse|True)$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?command=new&obj=[0-
9]{1,5}&tab=5&att=[01]&type=[017]&imp=[12]&IsSavedRegAppt=([Ff]alse|True)$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?command=new&obj=[0-
9]{1,5}&tab=[12]&att=[01]&type=[017]&IsSavedRegAppt=([Ff]alse|True)$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?command=new&obj=[0-
9]{1,5}&tab=[12]&att=[01]&type=[017]&imp=[12]&IsSavedRegAppt=([Ff]alse|True)$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?command=new&obj=[0-
9]{1,5}&tab=[12]57&att=[01]&type=[017]&imp=[12]&IsSavedRegAppt=([Ff]alse|True)$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?obj=[0-9A-
F]{220}&command=editseries&tab=[12]&att=[01]&imp=0&type=[017]&IsSavedRegAppt=([Ff]alse|T
rue)$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?obj=[0-9A-
F]{220}&command=read&tab=[12]&att=[01]&imp=0&type=[017]&IsSavedRegAppt=([Ff]alse|True)$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?obj=[0-9A-
F]{220}&command=read&tab=[12]&att=[01]&imp=[12]&type=[017]&IsSavedRegAppt=([Ff]alse|True
)$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?obj=[0-
9]{1,5}&command=new&tab=4&att=[01]&IsSavedRegAppt=([Ff]alse|True)&imp=[12]&type=[017]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrTitle.asp?obj=[0-
9]{1,5}&command=new&tab=[12]&att=[01]&imp=[12]&type=[017]&IsSavedRegAppt=([Ff]alse|True)
$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrtitle.asp?command=editseries&obj=[0-
9A-F]{220}&tab=[12]&att=[01]&type=[017]&IsSavedRegAppt=([Ff]alse|True)&imp=[12]$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrtitle.asp?command=read&obj=[0-9A-
F]{220}&tab=[12]&att=[01]&type=[017]&IsSavedRegAppt=([Ff]alse|True)&imp=0$"
EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/request/mrtitle.asp?command=read&obj=[0-9A-
F]{220}&tab=[12]&att=[01]&type=[017]&IsSavedRegAppt=([Ff]alse|True)&imp=[12]$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/resp/commands.asp?obj=[0-9]{1,5}$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/resp/frmRoot.asp?obj=[0-
9]{1,5}&cancelMR=2&replyMR=0$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/resp/rspMsg.asp?obj=[0-
9]{1,5}&caller=1&milTime=0&replyMR=0&replyCancel=0$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/resp/rspTitle.asp?tab=[12]&att=[01]&imp=[12]&ms
gType=0&cancelMR=2$"

EAccessRule permit "^GET
/exchange/USA/forms/ipm/schedule/meeting/resp/rsptitle.asp?tab=[12]&att=[01]&imp=[12]&ms
gType=0&cancelMR=2$"

EAccessRule permit "^GET /exchange/USA/forms/low.gif$"

EAccessRule permit "^GET /exchange/USA/forms/mailcont.gif$"

EAccessRule permit "^GET /exchange/USA/forms/movcpy.gif$"

EAccessRule permit "^GET /exchange/USA/forms/mtgaccpt.gif$"

EAccessRule permit "^GET /exchange/USA/forms/mtgcont.gif$"

EAccessRule permit "^GET /exchange/USA/forms/mtgdecln.gif$"

EAccessRule permit "^GET /exchange/USA/forms/mtgtent.gif$"

EAccessRule permit "^GET /exchange/USA/forms/nextmsg.gif$"

EAccessRule permit "^GET /exchange/USA/forms/prevmsg.gif$"

EAccessRule permit "^GET /exchange/USA/forms/reply.gif$"

EAccessRule permit "^GET /exchange/USA/forms/replyall.gif$"

EAccessRule permit "^GET /exchange/USA/forms/resolve.gif$"

EAccessRule permit "^GET /exchange/USA/forms/save.gif$"

EAccessRule permit "^GET /exchange/USA/forms/send.gif$"

EAccessRule permit "^GET /exchange/USA/forms/showmap.gif$"

EAccessRule permit "^GET /exchange/USA/forms/tabWdot.gif$"

EAccessRule permit "^GET /exchange/USA/forms/tablcor.gif$"

EAccessRule permit "^GET /exchange/USA/forms/tabrcor.gif$"

EAccessRule permit "^GET /exchange/USA/forms/tabrline.gif$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
EAccessRule permit "^GET /exchange/USA/forms/viewcal.gif$"
EAccessRule permit "^GET /exchange/USA/help/calcalar.gif$"
EAccessRule permit "^GET /exchange/USA/help/calfrm.gif$"
EAccessRule permit "^GET /exchange/USA/help/calhelp.gif$"
EAccessRule permit "^GET /exchange/USA/help/calnavbr.gif$"
EAccessRule permit "^GET /exchange/USA/help/calover.htm$"
EAccessRule permit "^GET /exchange/USA/help/calscdar.gif$"
EAccessRule permit "^GET /exchange/USA/images/arwtanlf.gif$"
EAccessRule permit "^GET /exchange/USA/images/arwtanrt.gif$"
EAccessRule permit "^GET /exchange/USA/images/calendar.gif$"
EAccessRule permit "^GET /exchange/USA/images/contact.gif$"
EAccessRule permit "^GET /exchange/USA/images/deleted.gif$"
EAccessRule permit "^GET /exchange/USA/images/delfoldr.gif$"
EAccessRule permit "^GET /exchange/USA/images/delmsg.gif$"
EAccessRule permit "^GET /exchange/USA/images/divider.gif$"
EAccessRule permit "^GET /exchange/USA/images/empfldr.gif$"
EAccessRule permit "^GET /exchange/USA/images/envelope.gif$"
EAccessRule permit "^GET /exchange/USA/images/folder.gif$"
EAccessRule permit "^GET /exchange/USA/images/help.gif$"
EAccessRule permit "^GET /exchange/USA/images/inbox.gif$"
EAccessRule permit "^GET /exchange/USA/images/low.gif$"
EAccessRule permit "^GET /exchange/USA/images/mailbox.gif$"
EAccessRule permit "^GET /exchange/USA/images/mark.gif$"
EAccessRule permit "^GET /exchange/USA/images/meeting.gif$"
EAccessRule permit "^GET /exchange/USA/images/mffav.gif$"
EAccessRule permit "^GET /exchange/USA/images/movcpy.gif$"
EAccessRule permit "^GET /exchange/USA/images/mtgcancl.gif$"
EAccessRule permit "^GET /exchange/USA/images/mtgreq.gif$"
EAccessRule permit "^GET /exchange/USA/images/ndr.gif$"
EAccessRule permit "^GET /exchange/USA/images/newappt.gif$"
EAccessRule permit "^GET /exchange/USA/images/newcont.gif$"
EAccessRule permit "^GET /exchange/USA/images/newfoldr.gif$"
EAccessRule permit "^GET /exchange/USA/images/newmail.gif$"
EAccessRule permit "^GET /exchange/USA/images/newmtg.gif$"
EAccessRule permit "^GET /exchange/USA/images/newpost.gif$"
EAccessRule permit "^GET /exchange/USA/images/outbox.gif$"
EAccessRule permit "^GET /exchange/USA/images/papclip.gif$"
EAccessRule permit "^GET /exchange/USA/images/prop.gif$"
EAccessRule permit "^GET /exchange/USA/images/recur.gif$"
EAccessRule permit "^GET /exchange/USA/images/refresh.gif$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
EAccessRule permit "^GET /exchange/USA/images/sent_itm.gif$"

EAccessRule permit "^GET /exchange/USA/images/upone.gif$"

EAccessRule permit "^GET /exchange/USA/images/urgent.gif$"



EAccessRule permit "^GET
/exchange/USA/inbox/commands.asp?action=(deleteallmessages|deletefolder)&obj=[0-9A-
F]{92}&store=[012]$"
EAccessRule permit "^GET
/exchange/USA/inbox/commands.asp?command=(deleteallmessages|deletefolder|checkmessages|n
ewfolder|nothing|updateview)&obj=[0-9A-F]{92}&s
tore=[012]$"
EAccessRule permit "^GET
/exchange/USA/inbox/commands.asp?command=(deleteallmessages|deletefolder|checkmessages|n
ewfolder|nothing|updateview)&store=[012]$"
EAccessRule permit "^GET
/exchange/USA/inbox/commands.asp?command=(deleteallmessages|deletefolder|checkmessages|n
ewfolder|nothing|updateview)&view=[0-9]&page=[0-9]{1,3}&obj=[0-9A-F]{92}&store=[012]$"
EAccessRule permit "^GET
/exchange/USA/inbox/commands.asp?store=[012]&command=newfolder$"

EAccessRule permit "^GET /exchange/USA/inbox/envelope.gif$"

EAccessRule permit "^GET
/exchange/USA/inbox/main_fr.asp?store=[012]&command=newfolder&obj=[0-9A-F]{92}$"
EAccessRule permit "^GET /exchange/USA/inbox/main_fr.asp?store=[012]&obj=$"
EAccessRule permit "^GET /exchange/USA/inbox/main_fr.asp?view=[0-
9]&store=[012]&obj=&acs=$"

EAccessRule permit "^GET /exchange/USA/inbox/messages.asp?obj=[0-9A-F]{92}&page=[0-
9]{1,3}$"
EAccessRule permit "^GET /exchange/USA/inbox/messages.asp?obj=[0-9A-F]{92}&page=[0-
9]{1,3}&view=[0-9]&compidx=[012]&store=[012]$"
EAccessRule permit "^GET /exchange/USA/inbox/messages.asp?obj=[0-9A-F]{92}&store=[012]$"

EAccessRule permit "^GET /exchange/USA/inbox/papclip.gif$"

EAccessRule permit "^GET /exchange/USA/inbox/peerfldr.asp?obj=[0-9A-F]{92}&store=[012]$"
EAccessRule permit "^GET /exchange/USA/inbox/peerfldr.asp?obj=[0-9A-
F]{92}&store=[012]&timedout=false$"

EAccessRule permit "^GET /exchange/USA/inbox/title.asp?compidx=[012]&store=[012]$"
EAccessRule permit "^GET /exchange/USA/inbox/title.asp?obj=[0-9A-
F]{92}&acs=&compidx=[012]&store=[012]$"
EAccessRule permit "^GET /exchange/USA/inbox/title.asp?page=[0-9]{1,3}&view=[0-
9]&compidx=[012]$"

EAccessRule permit "^GET /exchange/USA/inbox/urgent.gif$"

EAccessRule permit "^GET /exchange/USA/item.asp?action=next$"
EAccessRule permit "^GET /exchange/USA/item.asp?action=prev$"

EAccessRule permit "^GET /exchange/USA/logoff.asp$"

EAccessRule permit "^GET /exchange/USA/logon.asp$"
EAccessRule permit "^GET /exchange/USA/logon.asp?newwindow=1&viewer=1$"

EAccessRule permit "^GET /exchange/USA/msie.gif$"

EAccessRule permit "^GET /exchange/USA/msprod.gif$"

EAccessRule permit "^GET /exchange/USA/options/set.asp$"

EAccessRule permit "^GET /exchange/USA/part1.gif$"

EAccessRule permit "^GET /exchange/USA/part2.gif$"

EAccessRule permit "^GET /exchange/USA/relogon.htm$"

EAccessRule permit "^GET /exchange/USA/root.asp$"
EAccessRule permit "^GET /exchange/USA/root.asp?view=[0-9]&store=[012]&obj=$"
EAccessRule permit "^GET /exchange/USA/root.asp?view=[0-9]&store=[012]&obj=[0-9A-
F]{92}$"

EAccessRule permit "^POST
/exchange/USA/contacts/commands.asp?action=deletemarkedmessages$"

EAccessRule permit "^POST /exchange/USA/finduser/fumsg.asp$"
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
EAccessRule permit "^POST /exchange/USA/forms/IPM/CONTACT/commands.asp$"

EAccessRule permit "^POST /exchange/USA/forms/IPM/NOTE/commands.asp$"

EAccessRule permit "^POST /exchange/USA/forms/ipm/contact/commands.asp$"

EAccessRule permit "^POST /exchange/USA/forms/ipm/note/commands.asp$"
EAccessRule permit "^POST /exchange/USA/forms/ipm/note/commands.asp?tab=[12]57&obj=[0-
9]{1,5}&cc=1&rtn=m&bcc=0$"

EAccessRule permit "^POST
/exchange/USA/forms/ipm/schedule/meeting/request/commands.asp$"
EAccessRule permit "^POST
/exchange/USA/forms/ipm/schedule/meeting/request/commands.asp?att=[01]&type=[017]&imp=[1
2]&IsSavedRegAppt=([Ff]alse|True)&tab=[12]57&r
tn=r&obj=[0-9]{1,5}&cc=0$"

EAccessRule permit "^POST /exchange/USA/forms/ipm/schedule/meeting/resp/commands
.asp$"

EAccessRule permit "^POST /exchange/USA/inbox/commands.asp$"
EAccessRule permit "^POST /exchange/USA/inbox/commands.asp?action=deletemarkedmessages$"

EAccessRule permit "^POST /exchange/USA/options/set.asp$"

EAccessRule permit "^POST /exchange/exupload.dll$"
```

References

[1]Cisco Web site Internetworking Technology Overview
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm#10636

[2]John Pescatore, "Nimda Worm Shows You Can't Always Patch Fast Enough". Gartner report 19 September 2001,
http://www3.gartner.com/DisplayDocument?doc_cd=101034 (15 Oct 2001)

[3]Windows 2000 magazine Security Administrator poll in response to Gartner report
http://www.secadministrator.com/Poll/Index.cfm?Action=PollResults&Q_ID=695

[4]Steven Bonisteel Firms Should Pay More Attention To Web Security – Report, Newsbytes.,10 Oct 2001
http://www.newsbytes.com/news/01/170988.html (18 Oct 2001)

[5] William Cheswick and Stephen Bellovin. Firewalls and Internet Security. Repelling the Wily Hacker, What firewall's can't do, Addison-Wesley Reading, MA 1994 p.83

[6]Cisco web site Mailguard
http://www.cisco.com/warp/public/110/22.html (18 Oct 2001)

[7] Cisco web site Network Based Application Recognition
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e2/nbar2e.htm (18 Oct 2001)

[8] Cisco web site Using Network-Based Application Recognition and Access Control Lists for Blocking the "code red" worm at network ingress points
http://www.cisco.com/warp/public/63/nbar_acl_corered.shtml (18 Oct 2001)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

[9] Microsoft URLSCAN
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/urlscan.asp (18 Oct 2001)

[10] Installing the Apache-WebLogic Server Plug-in
http://www.weblogic.com/docs51/admindocs/apache_bridge.html (18 Oct 2001)

[11] RFC 3143 Known HTTP Proxy/Caching Problems
http://sunsite.dk/RFC/rfc/rfc3143.html (15 Oct 2001)

[12] nddconfig script for Solaris
http://www.sun.com/software/solutions/blueprints/tools/nddconfig (19 Oct 2001)

© SANS Institute 2001, Author retains full rights

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced