

RE: VPN's – Firewall's and Security

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-09/0273.html>

From: Christopher Joles (CJoles_at_proteabhs.com)

Date: 09/06/03

Date: Sat, 6 Sep 2003 08:20:14 -0400

To: "HOULE, FRANCIS" <francis.houle@bell.ca>, "Shota Gedenidze" <security@tub.ge>, <security-basi

Here is what we did to solve our delima

On the PIX we had an access list associated with the outside interface, we turned off sysopt connection permit ipsec and then added the following to the outside access-list:

```
access-list 102 permit tcp 192.168.18.0 255.255.255.0 192.168.0.0
255.255.255.0 eq smtp
access-list 102 permit tcp 192.168.18.0 255.255.255.0 192.168.0.0
255.255.255.0 eq pop3
access-list 102 permit tcp 192.168.18.0 255.255.255.0 192.168.0.0
255.255.255.0 eq 3389
access-list 102 permit tcp 192.168.18.0 255.255.255.0 192.168.0.0
255.255.255.0 eq www
access-list 102 permit tcp 192.168.18.0 255.255.255.0 192.168.254.0
255.255.255.0 eq www
access-list 102 permit tcp 192.168.18.0 255.255.255.0 192.168.254.0
255.255.255.0 eq 3389
access-list 102 permit tcp 192.168.18.0 255.255.255.0 192.168.254.0
255.255.255.0 eq pop3
access-list 102 permit tcp 192.168.18.0 255.255.255.0 192.168.254.0
255.255.255.0 eq smtp
access-list 102 permit ip 192.168.18.0 255.255.255.0 host 192.168.0.222
```

My original goal was to only allow ports 3389, 25, 110, and 80 over the VPN connections. What you see above does exactly that, along with the last line allowing dns and wins too.

Reading through the access list, 192.168.18.x is the subnet assigned to any outside VPN connection, 192.168.0.x is the private network and 192.168.254.x is the DMZ network.

I'd like to thank everyone for their help and assistance.

Christopher J. Joles
Chief Information Officer

SecurityFocus BASICS: RE: VPN's – Firewall's and Security

-----Original Message-----

From: HOULE, FRANCIS [mailto:francis.houle@bell.ca]
Sent: Wednesday, September 03, 2003 1:06 PM
To: 'Shota Gedenidze'; Christopher Joles;
security-basics@securityfocus.com
Subject: RE: VPN's – Firewall's and Security

You cannot use map [mapname] match address [access-list name] for VPN clients. Only for static crypto maps...

VPN clients uses dynamic crypto map and you cannot match traffic through access-list in those crypto's!!!!

Like I said, and this is confirmed by multiple SE's at cisco's, the only way to filter traffic from vpn clients is with X-auth...

--

Francis Houle
(514) 870-0388

-----Original Message-----

From: Shota Gedenidze [mailto:security@tub.ge]
Sent: Wednesday, August 27, 2003 2:53 AM
To: 'Christopher Joles'; security-basics@securityfocus.com
Subject: RE: VPN's - Firewall's and Security

Hi there,

Since you have vpn it is not firewalled!

You had configured that vpn users access internal network, You need to modify your PIX Config, you have configured "crypto map [mapname] match address [access-list name]"

You should modify that access-list and prohibit there following traffic:
Tcp/udp 135, 137, 139, 445

These ports are commonly used by rpc service.

Also block tftp protocol , tcp port 4444- this port is opened by blaster.

My advise:

Block everything and then allow ONLY important protocols you use.

In access-lists use permit tcp, permit udp, permit icmp rather than permit ip which is less specific.

Sincerely,

Shota Gedenidze.

-----Original Message-----

From: Christopher Joles [mailto:CJoles@proteabhs.com]
Sent: Tuesday, August 26, 2003 7:09 PM
To: security-basics@securityfocus.com
Subject: VPN's - Firewall's and Security

Good Day All!

I'm looking for design advice.

Currently, I have a network that is protected by a Cisco PIX 515 = firewall. We have it configured to protect our internal network along = with supplying access to our DMZ which holds our email and web servers. My concern arises from the spread of the blaster worm. Currently we = give a couple employees (the boss, the CFO and myself) VPN access from = home. In this scenario, the bosses home computer was compromised by the = blaster worm and luckily for me, he was on vacation in Germany at the = time. If he wasn't, he most assuridly would have made a VPN connection = and the lovely blaster worm would have gotten through our defenses. = Keep in mind, I had applied the MS patch to our servers and = workstations, however, it would have still gotten "inside". How can I = redesign my network to either firewall the VPN connections or at a =

RE: VPN's – Firewall's and Security

SecurityFocus BASICS: RE: VPN's – Firewall's and Security

minimum filter them.
Thanx for your opinions in advance!
Christopher J. Joles
Chief Information Officer
PROTEA Behavioral Health Services
187 Exchange St.
Bangor, ME 04401
Phone: (207)992-7010 Ext: 245 Fax:(207)992-7011

Attend Black Hat Briefings & Training Federal, September 29-30
(Training),
October 1-2 (Briefings) in Tysons Corner, VA; the world's premier
technical IT security event. Modeled after the famous Black Hat event
in
Las Vegas! 6 tracks, 12 training sessions, top speakers and sponsors.
Symantec is the Diamond sponsor. Early-bird registration ends September
6.Visit us: www.blackhat.com

Attend Black Hat Briefings & Training Federal, September 29-30
(Training),
October 1-2 (Briefings) in Tysons Corner, VA; the world's premier
technical IT security event. Modeled after the famous Black Hat event
in
Las Vegas! 6 tracks, 12 training sessions, top speakers and sponsors.
Symantec is the Diamond sponsor. Early-bird registration ends September
6.Visit us: www.blackhat.com

Attend Black Hat Briefings & Training Federal, September 29-30
(Training),
October 1-2 (Briefings) in Tysons Corner, VA; the world's premier
technical IT security event. Modeled after the famous Black Hat event
in
Las Vegas! 6 tracks, 12 training sessions, top speakers and sponsors.
Symantec is the Diamond sponsor. Early-bird registration ends September
6.Visit us: www.blackhat.com

Captus Networks
Are you prepared for the next Sobig & Blaster?
- Instantly Stop DoS/DDoS Attacks, Worms & Port Scans
- Precisely Define and Implement Network Security
- Automatically Control P2P, IM and Spam Traffic
FIND OUT NOW - FREE Vulnerability Assessment Toolkit
<http://www.captusnetworks.com/ads/42.htm>