

Re: Outgoing IPSEC

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2005-11/0379.html>

From: Securi Net (securinet2004_at_yahoo.ca)

Date: 11/22/05

Date: Tue, 22 Nov 2005 11:29:10 -0500 (EST)

To: Jason Thompson <securitux@gmail.com>

Thanks again, Jason.

That clarifies it and gives me a strong case in denying such requests.

Thank you everyone for your responses.

Regards

CP

--- Jason Thompson <securitux@gmail.com> wrote:

> *No problem.*
>
> *With a stateful inspection device (firewall), it*
> *does allow*
> *bidirectional traffic as long as your client*
> *initiates the VPN*
> *connection to the endpoint. Once the client connects*
> *to the endpoint*
> *it creates a connection that your firewall*
> *recognizes as 'in state'*
> *and allows traffic between the two devices. This is*
> *by design. So with*
> *a stateful inspection firewall, even though you are*
> *creating rules*
> *that say allow only outbound from client to*
> *endpoint, you are*
> *essentially saying 'only the client is allowed to*
> *initiate a*
> *connection'. Once the client creates the tunnel,*
> *bidirectional traffic*
> *is permitted so long as it obeys the rules of IP*
> *"state" (same IP*
> *addresses, connection kept alive, in the case of*

SecurityFocus BASICS: Re: Outgoing IPSEC

- > *TCP: syn, syn/ack,*
- > *ack, push, push/ack, sequence numbers,*
- > *acknowledgement numbers, etc).*
- > *UDP state is also kept using timeouts, since UDP is*
- > *a stateless*
- > *protocol.*
- >
- > *Keep in mind, the ACTUAL TCP, UDP, and IP header (of*
- > *a tunnelled*
- > *connection) from a client or VPN endpoint is*
- > *encrypted / encapsulated*
- > *with a completely different header. So an IKE UDP*
- > *packet's*
- > *encapsulat*